OFFICE OF THE SECRETARY OF DEFENSE
1950 DEFENSE PENTAGON
WASHINGTON, DC 20301-1950

21 SEP 2007

ADMINISTRATION &
MANAGEMENT

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANT SECRETARIES OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Safeguarding Against and Responding to the Breach of Personally Identifiable Information

The Department of Defense has a continuing affirmative responsibility to safeguard Personally Identifiable Information (PII) in its possession and to prevent its theft, loss, or compromise. It is essential that all DoD personnel, to include its contractors and business partners, ensure their actions do not contribute to, nor result in, a compromise occurring if the Department is to retain the trust of those individuals on whom information is maintained.

While the DoD has adopted policies in this critical area, the Office of Management and Budget (OMB) has issued new requirements in the OMB Memorandum M-07-16 dated May 22, 2007, (http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf) . These requirements are intended to augment, and thereby strengthen, current agency programs.

This memorandum, establishes policy in Attachment 1 for the implementation of the new OMB requirements to the extent they are not presently incorporated in the current policies and procedures prescribed by DoD 5400.11-R, "DoD Privacy Program." The new DoD policies and procedures required by OMB and promulgated by this memorandum are effective immediately and are mandatory for all DoD Components. These shall be incorporated into a future revision of DoD Directive 5400.11 and DoD 5400.11-R, as appropriate.

My point of contact for any questions relating to these policies, this memorandum or for any other matters relating to the Defense Privacy Program is Mr. Samuel P. Jenkins, Director, Defense Privacy Office, who may be contacted at (703) 607-2943 or email at sam.jenkins@osd.mil.

Michael B. Donley
Director, Administration and Management
Department of Defense Senior Privacy Official

Attachment:
As stated

Policy on Safeguarding Personally Identifiable Information and Breach Notification

The Department of Defense (DoD), through the requirements provided in this attachment, hereby establishes new privacy policy for the Department. These policies are intended to strengthen existing standards for the protection of personally identifiable information while at the same time improving the decision making process relative to breach notification and reporting.

Part I. Definitions.

Current DoD Policy:

A. Personally Identifiable Information (PII), as set forth in DoD Directive 5400.11, para E2.e and DoD 5400.11-R, para DL1.14, is defined as follows:

"Personal Information. Information about an individual that identifies, links, relates, or is unique to, or describes him or her, e.g., a Social Security Number; age; military rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc. Such information is also known as personally identifiable information (i.e., information which can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, date and place of birth, mother's maiden name, and biometric records, including any other personal information which is linked or linkable to a specified individual)."

A number of the elements included in the above definition of PII are public information subject to release under the Freedom of Information Act and DoD 5400.7-R, DoD Freedom of Information Act Program, e.g., name, civilian grade, and salary. Other elements are For Official Use Only, but are commonly shared in the work environment, e.g., name, business phone, military rank. As such, releases of these items of information, in general, do not constitute a breach. In situations where name or other unique identifier is listed alone, the context in which the name or other unique identifier is listed must be considered and a determination of the risk (or harm) must be conducted to determine if (a) a breach has occurred, and (b) whether notification is required. For example, a general support office rolodex contains personally identifiable information (name, phone number, etc.) likely would not be considered sensitive if it were breached. However, the same information in a database of patients at a clinic which treats contagious disease likely would be considered sensitive information. In situations where this personal information is linked with a name, Social Security Number and other identifiers and direct identification is possible, a determination of the risk (or harm) must be conducted to determine if notification is required. The evaluation of risk and harm in relationship to the data elements involved and their context are discussed in Appendix A and Table 1.

B. DoD 5400.11-R defines "lost, stolen or compromised information," otherwise termed a breach" as follows:

"Actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such

information for an other than authorized purposes where one or more individuals will be adversely affected. Such incidents also are known as breaches."

New OMB Requirements:

OMB defines a "breach" as follows:

"A loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic."

OMB also stresses that "agencies should bear in mind that notification of a breach when there is little or no risk of harm might create unnecessary concern and confusion. Adverse affect, or risk of harm, is implicitly part of the OMB concept of breach and will be maintained in the DoD definition of breach.

New DoD Policy:

DoD Components are to utilize the factors outlined in Appendix A and Table 1, or other approved methodology, to make determinations of risk of harm associated with a breach (loss, theft or compromise) of PII.

Part II. Training.

Current DoD Policy:

DoD Directive 5400.11, para 5.4.3, provides that the Secretaries of the Military Departments and the Heads of DoD Components shall:

"Conduct training, consistent with the requirements of the Privacy Act, the provisions of the DoD Directive 5400.11 and DoD 5400.11-R for personnel assigned, employed, and detailed, including contractor personnel and individuals having primary responsibility for implementing the DoD Privacy Program."

DoD 5400.11-R, Chapter 7, outlines such training requirements, to include:

Para C7.3.1 "The training shall include information regarding information privacy laws, regulations, policies and procedures governing the Department's collection, maintenance, use, or dissemination of personal information. The objective is to establish a culture of sensitivity to, and knowledge about, privacy issues involving individuals throughout the Department";

Para C7.3.3 "Include Privacy Act training in other courses of training when appropriate. Stress individual responsibility and advise individuals of their rights and responsibilities under this Regulation to ensure that it is understood that, where personally identifiable information is involved, individuals should handle and treat the information as if it was their own"; and

Para C7.4.3 "Components shall conduct training as frequently as believed necessary so that personnel who are responsible for or are in receipt of information protected by the [Privacy Act] are sensitive to the requirements of this Regulation, especially the access, use, and dissemination restrictions. Components shall give consideration to whether annual training and/or annual certification should be mandated for all or specified personnel whose duties and responsibilities require daily interaction with personally identifiable information".

New OMB Requirements:

A. OMB now requires that agencies initially train employees and managers on their privacy and security responsibilities before such personnel are authorized access to agency information and information systems.

1. Though DoD 5400.11-R para C7.3.2.1. and C7.3.2.2 currently require orientation and specialized training be conducted, it does not provide that training will be a prerequisite before an employee or manager is permitted to access DoD systems.

2. OMB Training Guidelines. OMB requires that agencies instruct their personnel on their roles and responsibilities for collecting, maintaining, and disseminating Privacy Act information; on agency rules and procedures for implementing the Privacy Act; and on penalties for failing to comply with these requirements. Training programs can be

conducted formally (e.g., official classes/seminars/briefings) or informally (on-the-job training).

3. OMB requires annual refresher training be provided to ensure that the employee and manager, as well as contractor personnel, continue to understand their responsibilities. OMB further requires that all personnel with authorized access to personally identifiable information (managers, employees, contractors) annual sign a document clearly describing their responsibilities acknowledging their understanding.

New DoD Policy:

A. The new DoD policy shall be that (1) training and communication related to privacy and security must be job specific and commensurate with an individual's responsibilities; (2) training will be a prerequisite before an employee, manager, or contractor is permitted to access DoD systems; and (3) such training is now mandatory for affected DoD military personnel, employees and managers, and shall include contractors and business partners.

B. To meet these training requirements, DoD components shall ensure their personnel receive Privacy Act training, as follows:

Orientation Training. Training that provides individuals with a basic understanding of the requirements of the Privacy Act as it applies to the individual's job performance. The training shall be provided to personnel, as appropriate, and should be a prerequisite to all other levels of training.

Specialized Training. Training that provides information as to the application of specific provisions of this instruction to specialized areas of job performance. Personnel of particular concern include, but are not limited to personnel specialists, finance officers, special investigators, paperwork managers, public affairs officials, IT professionals, and any other personnel responsible for implementing or carrying out functions under this instruction.

Management Training. Training that provides managers and decision makers considerations that they should take into account when making management decisions regarding the PA Program.

Privacy Act Systems of Records Training. Ensure all individuals who work with a Privacy Act system of records are trained on the provisions of the Privacy Act systems of records notice and this instruction. Stress individual responsibilities and advise individuals of their rights and responsibilities under this instruction.

C. Annual refresher training shall be provided to ensure employees and managers, as well as contractor personnel, continue to understand their responsibilities. All personnel with authorized access to personally identifiable information (managers, employees, contractors) shall annually sign a document clearly describing their responsibilities acknowledging their understanding. The certification to acknowledge awareness of responsibilities shall also be used to document initial

training completion prior to granting access. Follow-on annual certification shall be executed at the completion of annual refresher training. It shall be retained either in the DoD Component's central electronic personnel record system or in the office to which the employee is assigned or, where contractor personnel are involved, the appropriate office of the DoD Component supported by the contract. If contractor employees access DoD personally identifiable information from remote sites, the office or component supported shall document and maintain these certificates. The certifications (example p. 6) shall be subject to inspection during reviews by DoD Component Privacy Officials or DoD Component's Inspectors General.

D. OMB acknowledges that the DoD, among other agencies, offer a minimum baseline of security awareness training as part of the Information Systems Security Line of Business. It is a change in DoD policy that DoD Components shall examine such training, and if not already included, shall expand their training materials and program to include specific privacy and security awareness segments to their privacy and security training program(s) as above. Training shall include rules of behavior and consequences when rules are not followed. Additional or advanced training should be provided commensurate with increased responsibilities or change in duties. DoD Components are encouraged to adopt the promotion of privacy and security responsibility awareness through use of daily or periodic tips, reminder messages and incentives for reporting risks. DoD Component Privacy Officials shall be consulted in the development of such training and reminders.

Certification of Initial/Annual Refresher Training

The certification may read as follows:

"This is to certify that I have received initial/annual refresher training on my privacy and security responsibilities. I understand that I am responsible for safeguarding personally identifiable information that I may have access to incident to performing official duties. I also understand that I may be subject to disciplinary action for failure to properly safeguard personally identifiable information, for improperly using or disclosing such information, and for failure to report any known or suspected loss or the unauthorized disclosure of such information."

_____	_____
(Signature)	(Print Name)
_____	_____
(Date)	(DoD Component/Office)

Part III. Review of Personally Identifiable Information (PII) Holdings.

Current DoD Policy:

It is DoD Policy to comply with OMB Circular A-130, Appendix I, para 3.a. (8) which requires agencies to:

Biennially review each Privacy Act system of records notices to ensure that it accurately describes the system of records.

Unless components have claimed an exemption for a specific Privacy Act system of records, this review necessarily includes a determination whether the records contained in the system are accurate, relevant, timely, and complete.

Agencies review all systems that contain PII, whether or not they qualify as Privacy Act system of records, for purposes of determining whether such records are accurate, relevant, timely, and complete.

New OMB Requirements:

OMB directs that agencies develop specific implementation plans and progress updates regarding the review of PII Holdings and to incorporate them into the agency's annual Federal Information Security Management Act (FISMA) Privacy Report.

Upon following this initial review, OMB also directs that agencies develop and make public a schedule by which they will periodically update the review of their holdings.

New DoD Policy:

As part of this year's instructions for FISMA privacy reporting, DoD Components will be required to:

-- Confirm that they have established, or are in the process of establishing, PII review plans;

-- Provide a schedule by which they will periodically update their review of their holdings following the initial review.

A. It shall be DoD policy that the DoD Information Technology Portfolio Repository (DITPR) identifies all Components' automated systems containing PII. DoD Component Privacy Officials and DoD Component CIOs must coordinate for purposes of identifying Information Owners (as defined by the National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, Revised June 2006) to ensure that the PII holdings for each system, whether or not subject to the Privacy Act, are accurate, relevant, timely, and complete except where, as pursuant to a Privacy Act exemption rule, this standard

need not be met. For DoD Components' non-automated systems, the DoD Components' inventory of Privacy Act system of records notices shall be reviewed in the same manner.

B. It shall be DoD policy that the Periodic updates required by OMB should be designed so that (1) IT systems containing PII shall be reviewed on the same annual cycle as required by Policy 4.8 of the Interim Department of Defense (DoD) Certification and Accreditation (C&A) Process Guidance (DIACAP), dated July 6, 2006; and (2) Privacy Act system of records notices shall be reviewed at least once every two years.

C. DoD Components shall report the results of the review of the systems, processes and holdings annually to the Defense Privacy Office on the established schedule for annual FISMA reporting.

DoD Directive 5400.11 and DoD 5400.11-R will be revised to address FISMA reporting, the requirement for the periodic review of PII holdings and efforts to reduce the use of Social Security Numbers, etc.

Part IV. Incident Reporting and Handling Requirements.

A. Agency Reporting Requirements

Current DoD Policy:

DoD 5400.11-R, para C10.6, sets forth the current DoD reporting requirements when there is breach of PII. Reporting of incidents is required when there is a loss, theft, or compromise of PII (i.e., a breach).

All breaches shall continue to be reported to US-CERT within one hour of discovering that a breach of PII has occurred, to the Senior DoD Component Official for Privacy within 24 hours, and the Defense Privacy Office within 48 Hours for use in further reporting.

New OMB Requirements:

OMB requires that issuing banks be notified if a breach occurs involving government-authorized credit cards.

Breaches subject to reporting and notification include both electronic systems and paper documents.

New DoD Policy:

DoD Component Privacy Officials are to ensure notification to their Component Head coincides with notification to the Defense Privacy Office.

Component's shall ensure that their reporting procedures are updated to include notification to banks when the breach involves the loss, theft, or otherwise compromise of government credit cards issued by a bank.

Reporting and Notifications will include breaches involving both electronic and paper documents.

B. External Breach Notification Requirements

Current DoD Policy:

DoD 5400.11-R, para C1.5, sets forth the current DoD external notification policy when there is a breach of PII. Except to the extent modified below, the current policy continues in effect.

New OMB Requirements:

The OMB requires that an agency's notification policy should consist of a number of elements and considerations some of which are addressed in the current DoD policy. OMB has introduced the requirement to evaluate the risk of harm associated with a breach.

Whether breach notification is required? The OMB guidance provides that a determination should only be made to notify after an assessment has been made as to the risk of harm and the level of risk that results from the loss, theft, or compromise of the data.

In general, the risk of harm to the individual is higher the greater the sensitivity of the data involved. For example, a name associated with a Social Security Number poses a higher risk and potential harm to the individual than a name associated with a subscription list. In effect, a name in one context may be less sensitive than a name in another context. Therefore, in evaluating the risk of harm, consider the data elements in light of their context and the potential harm that could result if the information was used in an unlawful manner. Also, loss or exposure of data to unauthorized personnel may not be a breach requiring notification if the information is properly protected through coding or encryption.

The level of risk will depend on the manner of the actual or suspected breach and the nature of the information involved. A theft of a laptop may be but a target of opportunity where the thief intends to sell the laptop without regard for any information it might hold, but a penetration of a protected IT system may be an intentional effort on the part of the hackers to steal information for unauthorized purposes.

New DoD Policy:

It shall be DoD policy that when making the determination of whether notification of breach is required, the DoD Component will assess the likely risk of harm caused by the breached information and then assess the relative likelihood of the risk occurring (risk level).

There are five factors that the DoD Component's will consider to assess the likely risk of harm (see Appendix A). The DoD Component will consider a wide range of harms, such as harm to reputation and the potential for harassment or prejudice, particularly when health or financial benefits information is involved in the breach. The DoD Component will bear in mind that notification when there is little or no risk of harm might create unnecessary concern and confusion. The DoD Component will document its rationale and the resulting "Risk Level" for not providing a notification if the risk assessment determines notification is not required. A DoD Privacy Risk Level Table is attached. Any Service or Component wishing to propose a more rigorous, alternative Risk Level Table or methodology must submit it for approval to the Defense Privacy Office.

C. Timeliness of the Notification.

Current DoD Policy:

It shall continue to be DoD policy that notification shall be made as soon as possible, but not later than 10 working days after the loss, theft, or compromise is discovered and the identities of the individuals ascertained, but that notification may be delayed for good cause (e.g., law enforcement authorities request delayed notification as immediate notification will jeopardize investigative efforts). When notification is not made within the 10 day period, the DoD Components shall inform the Deputy Secretary of Defense why notice was not provided within the 10 day period. (The OMB guidance states that agencies should provide notification without unreasonable delay, but consistent with the needs of law enforcement and national security.)

D. Source of the Notification.

Current DoD Policy:

The Deputy Secretary of Defense has designated the Director of Administration and Management as the DoD Senior Privacy Official responsible for discharging those responsibilities and duties associated with the Defense Privacy Program (DoDD 5400.11).

New OMB Requirements:

The OMB guidance provides that the notification should be made by the Agency Head or a Senior-level individual designated in writing to demonstrate that the breach has the attention of the senior leadership.

New DoD Policy:

It shall be DoD policy that notifications shall be made by the Head of the DoD Component or a senior-level individual who is in the chain of command for the organization where the loss, theft, or compromise occurred.

E. Contents of the Notification.

Current DoD Policy:

DoD 5400.11-R, para C1.5 and Appendix 2, establish requirements for notification of individuals when information is lost, stolen or compromised. The current DoD policy reflects many of the required elements, but not all (DoD 5400.11-R, para C1.5).

New OMB Requirements:

The notification should be provided in writing and should be concise, conspicuous, and in plain language. The notice should include the following elements:

-- a brief description of what happened, including the date(s) of the breach and of its discovery;

-- to the extent possible, a description of the types of personal information involved in the breach (e.g., full name, Social Security Number, date of birth, home address, account number, disability code, etc.);

-- a statement whether the information was encrypted or protected by other means if it is determined that such information would be beneficial and would not compromise the security of the system;

-- what steps individuals should take to protect themselves from potential harm, if any;

-- what the agency is doing to investigate the breach, to mitigate losses, and to protect against further breaches, and

-- who affected individuals should contact at the agency for more information, including a phone number, either direct or toll-free, email address, and postal address.

F. Means of Providing Notification.

New DoD Policy:

It shall be DoD Policy that notifications to individuals continue to comply with the requirement of DoD 5400.11-R and include the new elements provided in the new OMB requirements.

New OMB Requirement:

The new OMB requirement specifies notification by first-class mail as the primary means notification is accomplished. OMB recognizes that other means, such as telephone, email, and substitute notice, etc., may also be employed depending on the number of individuals affected, what contact information is available, and the urgency associated with a particular breach. OMB guidance further provides that, when effecting notification by mail, the front of the envelope should be labeled to alert the recipient to the importance of its contents, e.g., "Data Breach Information Enclosed" and that the envelope is marked with the identify of the DoD Component that suffered the breach.

OMB further notes that other government-wide services, such as USA Services, including toll free number of 1-800-Fedinfor and www.USA.gov, are already in place to provide support services as needed.

New DoD Policy:

It shall be DoD policy that the preferred method of notifications will be made by first-class mail, but that other means are acceptable if the DoD Component making the notification determines that another means is preferable and is reasonably assured that the affected individuals will be contacted. It also shall be DoD policy that a follow-up written notification will be given when telephonic notification is effected. It further shall be DoD policy that the envelope will be marked as provided by the OMB guidance.

It shall continue to be DoD policy that a generalized (substitute) notice be given to the potentially impacted population by whatever means the DoD Component believes is most likely to reach the impacted individuals if the DoD Component cannot readily identify the affected individuals or will not be able to reach the individuals (DoD 5400.11-R, para C1.5).

G. Who Receives Notification.

New OMB Requirement:

The OMB guidance provides, appropriately so, that the first consideration is to notify the affected individual, but that further consideration should be given to notifying possible other third parties, such as the media, when failure to do so may possibly erode public trust.

New DoD Policy:

It shall be DoD policy that media notifications be promptly prepared in cases where the breach is significant (i.e., impacting thousands of individuals, the PII is highly sensitive) and the risks and potential for harm to the individuals involved as a result of the breach are greater than the risks and potential for harm to the investigation as a result of public disclosure of the breach. The actions taken to inform the media are necessary to preserve the public's trust. Early preparation ensures the DoD Components can readily respond to a media inquiry or when determined necessary, release information to media organizations.

DoD Components are responsible for establishing a protocol to determine when a public affairs release on a breach should be made. The Heads of DoD Components will make the determination to release the public announcement.

APPENDIX A

Identity Theft Risk Analysis

Five factors to consider when assessing the likelihood of risk and/or harm:

1. Nature of the Data Elements Breached. The nature of the data elements compromised is a key factor to consider in determining when and how notification should be provided to affected individuals. For example, theft of a database containing individuals' names in conjunction with Social Security Numbers, and/or dates of birth may pose a high level of risk of harm, while a theft of a database containing only the names of individuals may pose a lower risk, depending on its context.

It is difficult to characterize data elements as creating a low, moderate, or high risk simply based on the type of data because the sensitivity of the data element is contextual. A name in one context may be less sensitive than in another context. In assessing the levels of risk and harm, consider the data element(s) in light of their context and the broad range of potential harms flowing from their disclosure to unauthorized individuals.

2. Number of Individuals Affected. The magnitude of the number of affected individuals may dictate the method(s) you choose for providing notification, but should not be the only determining factor for whether an agency should provide notification.

3. Likelihood the Information is Accessible and Usable. Upon learning of a breach, agencies should assess the likelihood personally identifiable information will be or has been used by unauthorized individuals. An increased risk that the information will be used by unauthorized individuals should influence the agency's decision to provide notification.

Depending upon a number of physical, technological, and procedural safeguards employed by the agency, the fact the information has been lost or stolen does not necessarily mean it has been or can be accessed by unauthorized individuals. If the information is properly protected by encryption, for example, the risk of compromise may be low to non-existent. In this context, proper protection means encryption has been validated by National Institute of Standards & Technology (NIST).

Agencies will first need to assess whether the breach involving personally identifiable information is at a low, moderate, or high risk of being used by unauthorized persons to cause harm to an individual or group of individuals. The assessment should be guided by NIST security standards and guidance. Other considerations may include the likelihood any unauthorized individual will know the value of the information and either use or sell the information to others.

4. Likelihood the Breach May Lead to Harm.

Broad Reach of Potential Harm. The Privacy Act requires agencies to protect against any anticipated threats or hazards to the security or integrity of records which could result in "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." Additionally, agencies should consider a number of possible harms associated with the

loss or compromise of information. Such harms may include the effect of a breach of confidentiality or fiduciary responsibility, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, the disclosure of address information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.

Likelihood Harm Will Occur. The likelihood a breach may result in harm will depend on the manner of the actual or suspected breach and the type(s) of data involved in the incident. Social Security Numbers and account information are useful to committing identity theft, as are date of birth, passwords, and mother's maiden name. If the information involved, however, is a name and address or other personally identifying information, the loss may also pose a significant risk of harm if, for example, it appears on a list of recipients patients at a clinic for treatment of a contagious disease.

In considering whether the loss of information could result in identity theft or fraud, agencies should consult guidance from the Identity Theft Task Force found at (whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf).

5. Ability of the Agency to Mitigate the Risk of Harm. Within an information system, the risk of harm will depend on how the agency is able to mitigate further compromise of the system(s) affected by a breach. In addition to containing the breach, appropriate countermeasures, such as monitoring system(s) for misuse of the personal information and patterns of suspicious behavior, should be taken. Such mitigation may not prevent the use of the personal information for identity theft, but it can limit the associated harm. Some harm may be more difficult to mitigate than others, particularly where the potential injury is more individualized and may be difficult to determine.

Table 1. Risk Assessment Model

No.	Factor	Risk Determination	Low: Moderate: High:	Comments: All breaches of PII, whether actual or suspected, require notification to US-CERT Low and moderate risk/harm determinations and the decision whether notification of individuals is made, rest with the Head of the DoD Component where the breach occurred All determinations of high risk or harm require notifications
1.	What is the nature of the data elements breached? What PII was involved?			
	a. Name only	Low		Consideration needs to be given to unique names; those where one or only a few in the population may have or those that could readily identify an individual, i.e., public figure
	b. Name plus 1 or more personal identifier (not SSN, Medical or Financial)	Moderate		Additional identifiers include date and place of birth, mother's maiden name, biometric record and any other information that can be linked or is linkable to an individual
	c. SSN	High		
	d. Name plus SSN	High		
	e. Name plus Medical or Financial data	High		
2.	Number of Individuals Affected			The number of individuals involved is a determining factor in how notifications are made, not whether they are made
3.	What is the likelihood the information is accessible and usable? What level of protection applied to this information?			
	a. Encryption (FIPS 140-2)	Low		
	b. Password	Moderate/High		Moderate/High determined in relationship to category of data in No. 1
	c. None	High		
4.	Likelihood the Breach May Lead to Harm	High/Moderate/Low		Determining likelihood depends on the manner of the breach and the type(s) of data involved
5.	Ability of the Agency to Mitigate the Risk of Harm			
	a. Loss	High		Evidence exists that PII has been lost; no longer under DoD control
	b. Theft	High		Evidence shows that PII has been stolen and could possibly be used to commit ID theft?
	c. Compromise			
	(1) Compromise w/I DoD control	Low High		No evidence of malicious intent Evidence or possibility of malicious intent
	(2) Compromise beyond DoD control	High		Possibility that PII could be used with malicious intent or to commit ID theft

DoD Components are to thoroughly document the circumstances of all breaches of PII and the decisions made relative to the factors above in reaching their decision to notify or not notify individuals.